REMARKS/ARGUMENTS

1. Claims

Claims 33-61 are pending in the application. Claims 33, 48, 54-56 and 59 have been amended to distinguish the claims from *Wentker et al.* (WO 00/25278) referred to hereinafter as Wentker. Wentker fails to disclose all of the elements of the present invention. In particular, Wentker fails to disclose the features of:

> ...receiving a header message from a loading station by a mobile terminal *wherein the header message includes the header data having a cryptographic data item including a cryptographic checksum based on a message digest of the message calculated by a hash function*;
>
> and
>
> accepting the payload data by the mobile terminal conditioned on a verification process based on the header data, wherein the payload data is divided into a number of blocks of payload data *and the blocks of payload data do not carry authentication information*;

In particular, the smart card of Wentker receives a load command and a subsequent load file where the load file may comprise a plurality of data authentication pattern (DAP) blocks and one data block. However, a secure loading of large applications while securing the authenticity and integrity of the individual blocks as well as the entire package is not addressed in Wentker. Wentker discloses a load command that is being authenticated and then there follows one or more payload messages/applications where each such message has a DAP. This is technically different from the present invention wherein the first header has in its signature field the hash of a list of message digests (MDL in step 821) of the payload blocks P1 thru PN which is sent prior to sending the payload blocks. Thus the payload blocks do not to carry any authentication information at all in contrast to Wentker wherein the payload blocks each have a DAP.

Hence in the present invention, an MDL is created and protected by the header and the payload blocks are sent as they are. In contrast, in Wentker the payload block

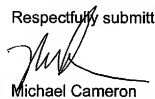
must be mapped onto messages that are each given a DAP. In the present invention, the chain of payloads are linked to the header in the sense that the blocks in the chain of payload blocks following after two different headers cannot be switched (when they differ). This is a result from the fact that the MDi values depend not only from the Pi but also from the previous payloads. In Wentker, the DAPs are created per payload as discussed at pages 21 and 22. Hence, the present invention differs technically from Wentker in how verification is realized and in what it achieves. In particular, the present invention the protection of the payloads is cryptographically linked to the header.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



Michael Cameron
Registration No. 50,298

Date: February 4, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-4145
michael.cameron@ericsson.com